資料2

米国等のサイバーセキュリティに関する動向

2015年3月17日

IPA　ニューヨーク事務所
JETRO　ニューヨーク事務所
八山幸司

1．サイバーセキュリティに関する最近のトピック

2．米国政府の施策

3．ユーザー企業のセキュリティ対策

4．サイバー保険の動向

最近の米国のサイバー攻撃の案件

●ホワイトハウス（2014年10月）
ホワイトハウスの機微でないネットワークがハッキング。ロシアの攻撃の可能性があるが、ホワイトハウスは何ら表明せず。

●ソニー・ピクチャー・エンターテイメント（2014年11月）
「平和の守護者（Guardians of Peace）」によるハッキング（被害額は3500万ドル）。政府は北朝鮮の攻撃と断定。

●米国中央軍（2015年1月）
米国中央軍のツイッターやユーチューブがハッキング。「イスラム国（ISIS）」の犯行声明。

●アンセム保険（2015年2月）
不正アクセスで顧客・従業員8000万人分の氏名、誕生日、社会保障番号、住所、電子メールのアドレス、収入などの雇用情報が流出。

（参考：2014年 9月ﾎｰﾑﾃﾞﾎﾟ社 5600万枚のカード情報流出、
2013年11～12月ﾀｰｹﾞｯﾄ社 4000万件のカード情報、7000万人分の個人情報流出）

オバマ政権におけるサイバーセキュリティ戦略

ブッシュ政権の政策を受けて
・ホワイトハウスにサイバーセキュリティ調整官を設置（2009年）
・全米サイバーセキュリティ教育イニシアチブ（NICE）を発表（2011年） など

2012年
サイバー脅威に関する情報共有などを進めるサイバーセキュリティ法策定を目指したが、情報提供の義務化などへの反発から廃案

2013年2月一般教書演説（オバマ2期）
ｻｲﾊﾞｰｾｷｭﾘﾃｨ強化に向けた大統領令、大統領指令
・今後官民で課題抽出
・必要な法制度の検討
・技術的なｿﾘｭｰｼｮﾝ策定
・ｻｲﾊﾞｰ関連情報を関係者で共有し重要情報をﾌｨｰﾄﾞﾊﾞｯｸする情報連携制度
・サイバーセキュリティ・フレームワークの創設（NIST作成、DHS運用）
→現行制度前提なので民間事業者の情報提供も任意

2015年1月13日に、新たなサイバーセキュリティに関する提案を発表
民間部門・政府間でのサイバーセキュリティ情報共有を改善、サイバー犯罪と闘う法執行機関の近代化、国家データのセキュリティ侵害に関して報告することを提案

米国連邦政府の体制

ホワイトハウス
サイバーセキュリティ調整官（Cybersecurity Coordinator）（2009年～）
国家のサイバーセキュリティ戦略・活動を統括する責任者
初代：ハワード・シュミット氏
（マイクロソフト等や、911後は政府でセキュリティ責任者）
現在：マイケル・ダニエル氏（元米行政管理予算局）

国土安全保障省（DHS）
サイバースペースの保護と安全性確保。重要インフラやITシステムのサイバーセキュリティ、サイバー関係の研究開発
国家サイバーセキュリティ通信統合センター（NCCIC；National Cybersecurity and Communications Integration Center ）：重要インフラ等のサイバー情報集約機関。US-CERT等を統括

国立標準技術研究所（NIST）
サイバーセキュリティの研究開発、人材育成
サイバーセキュリティ・フレームワークの策定

国防省（DOD）
サイバー司令部：陸海空等の各組織のサイバー部隊を統合し、米国軍のITインフラへの攻撃に対応。さらにはサイバースーペース全体のセキュリティ強化、米国民の保護など）。
司令官は国家安全保障局（NSA)長官が兼務（現在キース・アレキサンダー陸軍大将）
国家安全保障局（NSA）：諜報活動

連邦捜査局（FBI）
捜査、監視活動

サイバーセキュリティの情報共有の仕組み

サイバー脅威情報統合センター

（Cyber Threat Intelligence Integration Center (CTIIC)）

・オバマ大統領の今年の一般教書演説を受け、米国のサイバーセキュリティを強化するためのホワイトハウス主導による構想。
（2月10日にリサ・モナコ大統領補佐官がワシントンの講演で発表）

・テロ対策として設置された国家テロ対策センター（National Counter-Terrorism Center (NCTIC)）とならび、連邦捜査局（FBI）、中央情報局（CIA）、国家安全保障局（NSA）等の情報を一元的に集約し、分析結果を共有することでサイバー攻撃を防ぐことを目指す
（ソニー事件が本センター構想の推進力となった）

＜センター概要＞
・国家情報長官オフィス（ Office of the Director of National Intelligence； ODNI）の一部として設置予定。
・多種多様のデータ源や情報源から得たデータや情報を横断的に集めて、政府機関の間と民間とのデータの流れを安全に保つことが任務。
・ODNIを通じ、ホワイトハウス等に、各機関の情報を統合した単一情報をレポートする役割を担う予定。
・規模は、スタッフ約50人、予算は約3500万ドル（約40億円）の予定。

サイバーセキュリティの情報共有の仕組み

情報共有分析機関

（ISAOs; Information Sharing and Analysis Organizations）

・2月13日の大統領令で決定

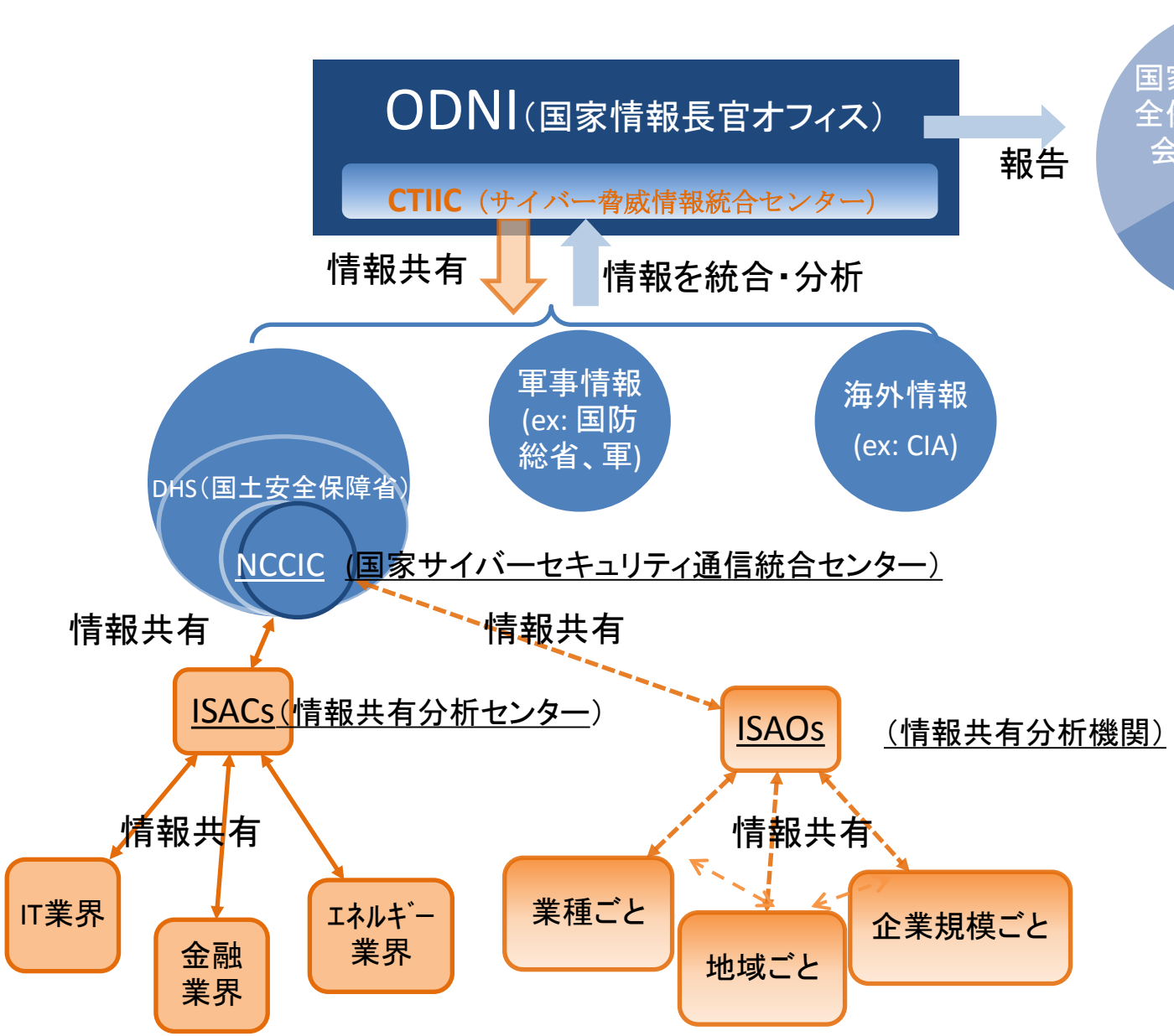
・各分野や地域毎に、「ISAOs（情報共有分析機関）」という団体を組織して、政府と民間の情報共有の接点の役目を担わせる。ISAOsは民間主導で、NPO、企業メンバー、又は民間の1企業など様々な形態が考えられる。

（注：類似の既存組織として、「情報共有分析センター」（ISACs; Information sharing and analysis center）。これは重要インフラ分野に対する物理・サイバー攻撃に対する脅威・脆弱性に関する情報共有を行うセンターであり、金融、エネルギー等セクター毎におかれ、一部はDHS（国土安全保障省）が運営。ISAOsとISACsは、相互補完的なものになると思われる）

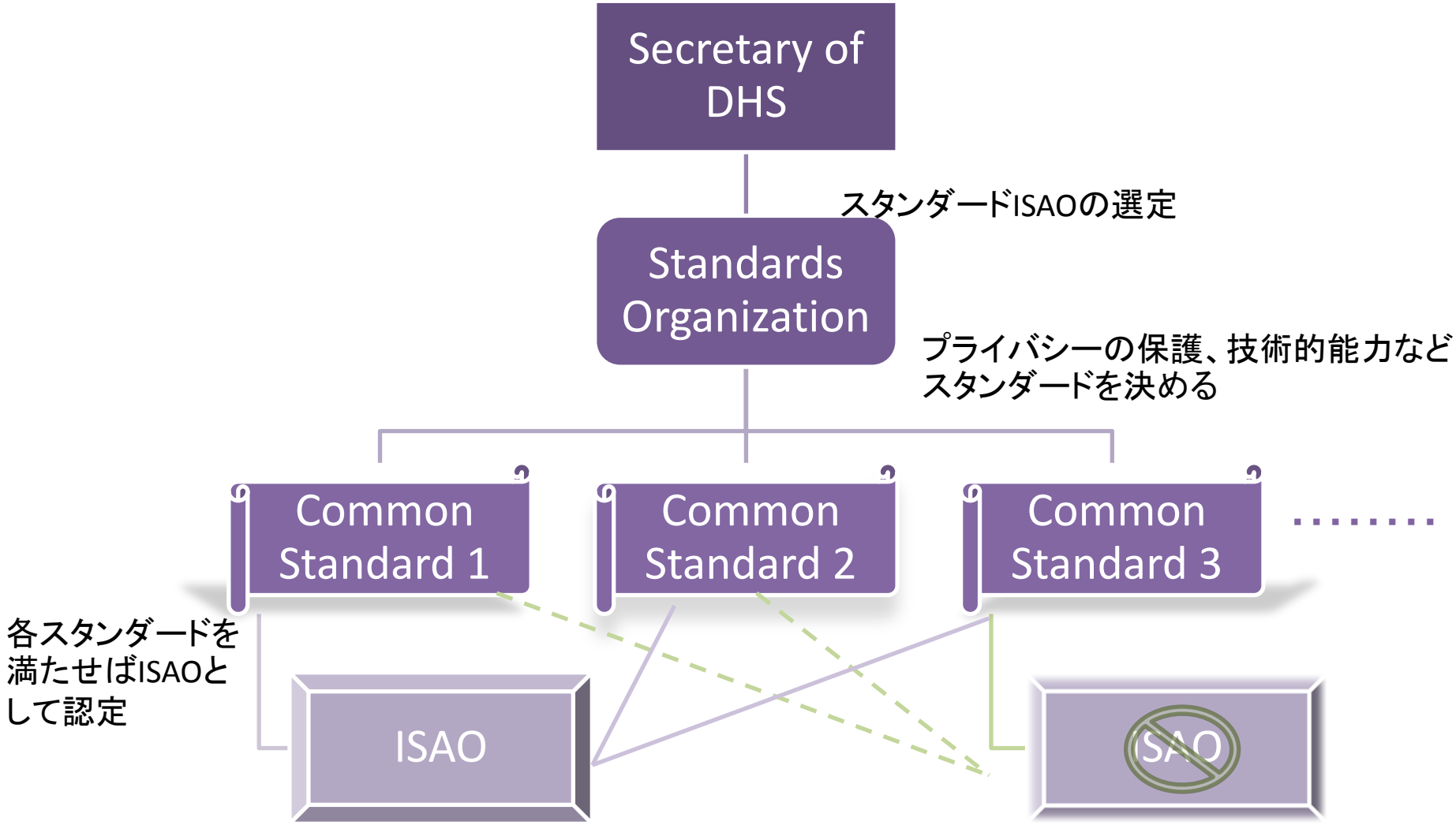
・ISAOsはDHS（国土安全保障省）傘下の国家サイバーセキュリティ通信統合センター（NCCIC；National Cybersecurity and Communications Integration Center ）と連携しながら活動を行う。

・今後ISAOsの中からスタンダードISAOsを選定し、ここが情報共有の仕組みのスタンダードを作っていく。

サイバーセキュリティの情報共有の仕組み



「情報共有分析機関」（ISAOs; Information Sharing and Analysis Organizations）の選定の仕組み



官民連携の取り組み

官民連携R&Dｾﾝﾀｰ（NCCoE: National Cybersecurity Center of Excellence ）

NISTがﾒﾘｰﾗﾝﾄﾞ大学内部に設置（2012年2月～）

以下を目標に研究開発を実施

・安全でプライバシーに配慮した情報技術のためのセキュリティ標準・基準などの基盤策定。

・コンピュータや企業システムのセキュリティのあり方を策定・モニタリング・測定方法を開発・テスト。

・官民全体に適用できる実用的かつ有用なサイバーセキュリティ機能を幅広く適用。

米国サイバー・チャレンジ（US Cyber Challenge）

官民合同のサイバーセキュリティ人材育成プログラム

非営利団体のNational Board of Information Security Examiners (NBISE)が運営

→サイバーセキュリティの合宿型講習会Cyber Campや、サイバー技術競技大会CyberQuestなどを実施

サイバーセキュリティ・フレームワーク

2013年2月、重要インフラのサイバーセキュリティ強化に向けた大統領令を受け、
2014年2月、NIST（国立標準技術研究所）が「重要インフラのサイバーセキュリティを向上させるためのフレームワーク」を策定。

以下の3つの要素から構成

①フレームワークコア（Framework Core）:
　全ての重要インフラ分野に共通となるサイバーセキュリティ対策のベストプラクティス、期待される成果、適用可能な参考情報など

②フレームワークインプレメンテーションティア（Framework Implementation Tiers）:
　企業がサイバーセキュリティリスクをどのようにとらえ、そのリスクを管理するために実施するプロセス

③フレームワークプロファイル（Framework Profile）:
　本フレームワークのカテゴリーから企業が選択することで、実際のビジネスニーズを基にした期待される成果

本アプローチで各企業がサイバーセキュリティのリスク管理を行いリスク低減を図ることを目標とする

本フレームワークの活用法

ステップ1: 優先順位付けを行い、範囲を決定する
ステップ2: 方向付けを行う
ステップ3:「現在のプロファイル」を作成する
ステップ4: リスクアセスメントを実施する
ステップ5:「目標のプロファイル」を作成する
ステップ6: ギャップを特定・分析し、優先順位付けを行う
ステップ7: 行動計画を実施する

（IPAの仮訳より（https://www.ipa.go.jp/files/000038957.pdf））

フレームワークコアの項目

特定 Identify	-資産管理	（ex.企業内の物理デバイスとシステムの一覧を作成している）
	- ビジネス環境	（ex.サプライチェーンにおける企業の役割を特定し伝達している）
	- ガバナンス	（ex.自組織の情報セキュリティポリシーを定めている）
	- リスクアセスメント	（ex.資産の脆弱性を特定し、文書化している）
	- リスク管理戦略	（ex.リスク管理プロセスが自組織の利害関係者によって確立、管理され、承認されている）
防御 Protect	- アクセス制御	（ex.承認されたデバイスとユーザの識別情報と認証情報を管理している）
	- 意識向上およびトレーニング	（ex.すべてのユーザに情報を周知しトレーニングを実施している）
	- データセキュリティ	（ex.保存されているデータを保護している）
	- 情報を保護するためのプロセスおよび手順	（ex.情報技術／産業用制御システムのベースラインとなる設定を定め、維持している）
	- 保守	（ex.自組織の資産の保守と修理は、承認・管理されたツールを用いて、タイムリーに実施し、ログを記録している）
	- 保護技術	（ex.ポリシーに従って監査記録／ログ記録の対象を決定、文書化し、そうした記録を実施して、レビューしている）

フレームワークコアの項目（続き）

検知 Detect	- 異常とイベント	（ex.ネットワーク運用のベースラインと、ユーザとシステム間の予測されるデータの流れを特定し、管理している）
	- セキュリティの継続的なモニタリング	（ex.発生する可能性のあるサイバーセキュリティイベントを検知できるよう、ネットワークをモニタリングしている）
	- 検知プロセス	（ex.説明責任を果たせるよう、検知に関する役割と責任を明確に定義している）
対応 Respond	- 対応計画の作成	（ex.イベントの発生中または発生後に対応計画を実施している）
	- 伝達	（ex.対応が必要になった時の自身の役割と行動の順番を従業員は認識している）
	- 分析	（ex.検知システムからの通知を調査している）
	- 低減	（ex.インシデントを封じ込めている）
	- 改善	（ex.学んだ教訓を対応計画に取り入れている）
復旧 Recover	- 復旧計画の作成	（ex.イベントの発生中または発生後に復旧計画を実施している）
	- 改善	（ex.学んだ教訓を復旧計画に取り入れている）
	- 伝達	（ex.広報活動を管理している）

フレームワーク・インプレメンテーション・ティアの項目

ティアは、企業がサイバーセキュリティリスクをどのようにとらえ、リスク管理するためにどのようなプロセスを実施しているかを示す指標。
ティア1(「部分的である」)からティア4(「適応している」)まで4段階に分類

ティア1: 部分的である(Partial)
- リスク管理プロセスは場当たり的で事後対処
- セキュリティリスクの管理が組織全体で未確立
- 外部関係者と協調または協力し合うためのプロセスを持っていない

ティア2: リスク情報を活用している(Risk Informed)
- リスク管理対策は経営層に承認されているが、企業全体で未確立
- セキュリティリスク意識はあるが、リスク管理するための組織全体の取組は未確立
- エコシステムにおける自組織の役割は理解しても、外部との共有能力は未確立

ティア3: 繰り返し適用可能である(Repeatable)
- 企業のリスク管理対策は正式に承認され、定期的に更新されている
- セキュリティリスク管理の取り組みが企業全体で確立、レビューされている
- 自組織の依存関係とパートナーを把握し、情報を得ており、セキュリティイベント時に協力関係

ティア4: 適応している(Adaptive)
- 過去と現在のセキュリティ対策から教訓を生かしセキュリティ対策を調整。継続的に改善
- セキュリティリスク管理が組織文化の一部となり、継続的にモニタリングし改善
- セキュリティイベント発生前に、セキュリティ向上のため、パートナーと積極的に情報共有

フレームワークに基づくインセンティブ

NISTのフレームワークを民間が導入しやすくするため、財務省、商業省、国土安全保障省（DHS）において様々なインセンティブを検討中

検討中の主なインセンティブ

●情報提供に関する安全性

企業がサイバーセキュリティに関する情報を、情報共有のために提供する場合、その情報の扱いや情報又は情報提供者の保護等に関して政府が責任を持つ。

●研究開発グラント

研究開発のグラントを申し込んでいる企業や組織に対して、フレームワークへの導入が行われていれば、導入の程度に応じて審査のポイントを与える。

●技術的なサポート

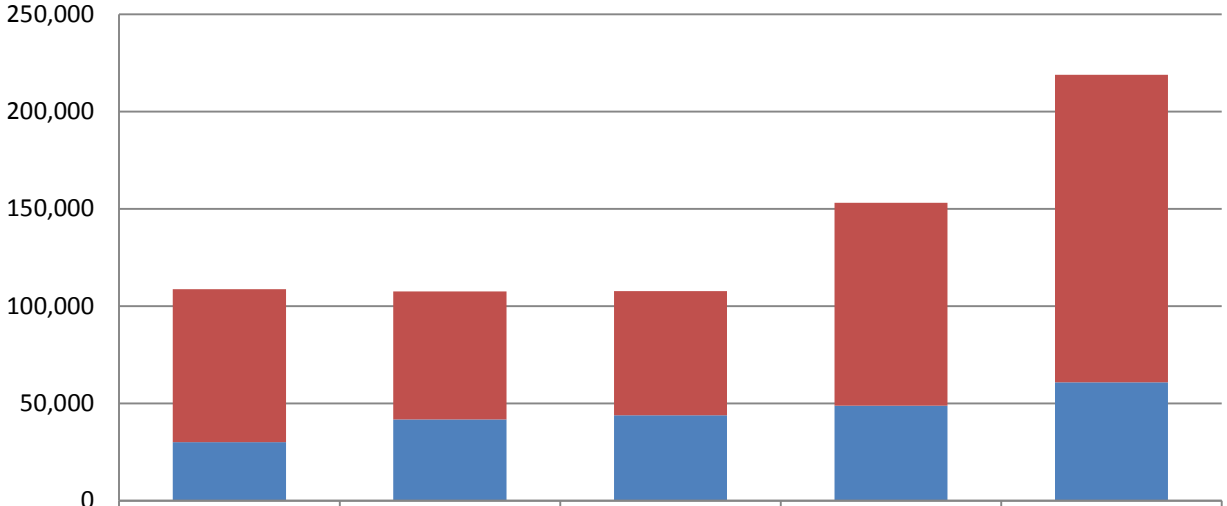
フレームワークの導入のためのアドバイスや指導等の機会を増やす。特に中小企業向け。

その他に、税制上の優遇措置なども検討中だが、課題も多い（規制や処罰もセットにすべき等様々な意見あり）

米国のサイバー攻撃の推移

米国におけるサイバー攻撃は近年急増している。特に民間部門への攻撃が急増している。

Cyber Incidents[1] in the US by Fiscal Year[2]



	2009	2010	2011	2012	2013
Other*	78,710	65,663	63,766	104,201	158,133
Federal Government	30,000	41,776	43,889	48,842	60,753

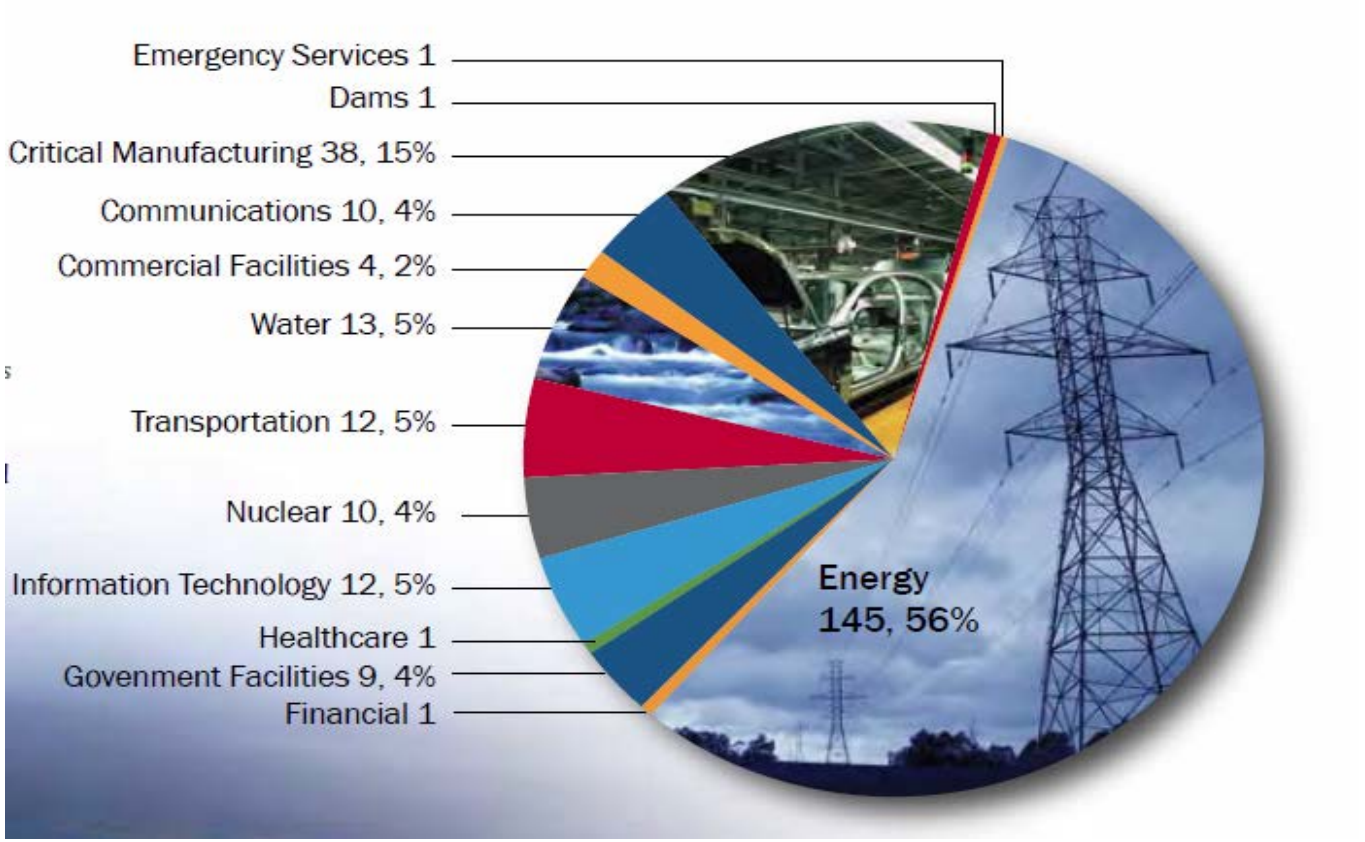
*Affecting state/Local governments, businesses and companies, and U.S. citizens

[1] United States Computer Emergency Readiness Team (US-CERT)への報告数
[2] 米国会計年度　10月1日～翌年9月30日

出典: 米国国土安全保障省(Department of Homeland Security) 連邦情報セキュリティマネジメント法（FISMA）年次報告書

米国の重要インフラへのサイバー攻撃

重要インフラ（エネルギー、金融、輸送機関、通信など）へのサイバー攻撃も多く、2013年ICS-CERTに報告された257件のサイバー攻撃のうち56%がエネルギー分野。
攻撃の種類も、不正アクセス、マルウェア、フィッシング等多様。



出典：ICS-CERT, “Year-in-Review”, 2013

世界の企業の規模・業種別サイバー攻撃の状況

ベライゾン社が世界27か国（日本を含む）で実施したサイバー攻撃の被害に関する調査によると、業種別では金融業界が最も被害数が多く、同業界では大企業の被害数が多い。次に多い業種は小売り、フードサービスであるが同業界では小企業の被害数が多い。

	Agriculture (11)	Mining (21)	Utilities (22)	Construction (23)	Manufacturing (31)	Wholesale Trade (42)	Retail (44)	Transportation (48)	Information (51)	Finance (52)	Real Estate (53)	Professional (54)	Management (55)	Administrative (56)	Educational (61)	Healthcare (62)	Recreation (71)	Accommodation (721)	Food Services (722)	Other Services (81)	Public (92)	Unknown	Total
1 to 100		1		2	10	1	79		5	18		14		3	1	3		3	38	6	2	7	193
101 to 1,000					13		3	1	8	3		5		1	2	1			13	2	4	1	57
1,001 to 10,000			1		7	1	3	22	10	12		6		1	2	1			2	1	2		71
10,001 to 100,000			2		13	1	4		2	93		5				1					1		122
More than 100,000		1	4		2					31		1					2		1				42
Unknown					1		7	1	14	73	1	5		1				1	2	2	5	23	136
Total		2	7	2	46	3	96	24	39	230	1	36		6	5	6	2	4	56	11	14	31	621

* Industries based on NAICS

出典：Verizon, “2013 Data Breach　Investigations Report"

世界の企業のサイバーセキュリティに関するデータ

PwC調査（2014年3～5月に世界の9700社以上を対象に実施）より
（企業の分類：北米35%, 欧州34%, アジア太平洋14%, 南米13%, アフリカ中近東4%）

・大企業ほど、被害数・被害規模とも増加

企業規模（売上規模別）	被害数		平均被害額	
	2013年	2014年	2013年	2014年
大企業（10億ドル以上）	9,155件	13,138件	390万ﾄﾞﾙ	590万ﾄﾞﾙ
中企業（1-10億ドル）	2,581件	4,227件	100万ﾄﾞﾙ	130万ﾄﾞﾙ
小企業（1億ドル以下）	1,151件	1,091件	65万ﾄﾞﾙ	41万ﾄﾞﾙ

・地域別被害数では欧州が急増（2013年から欧州41%増、北米11%増、アジア5%増、南米9%減）

・企業幹部のセキュリティ活動への関与が少ない
　幹部の関与：　セキュリティ組織・役割の見直し20%
　　現在のセキュリティリスクの見直し25%
　　セキュリティ技術30%
　　セキュリティ政策36%

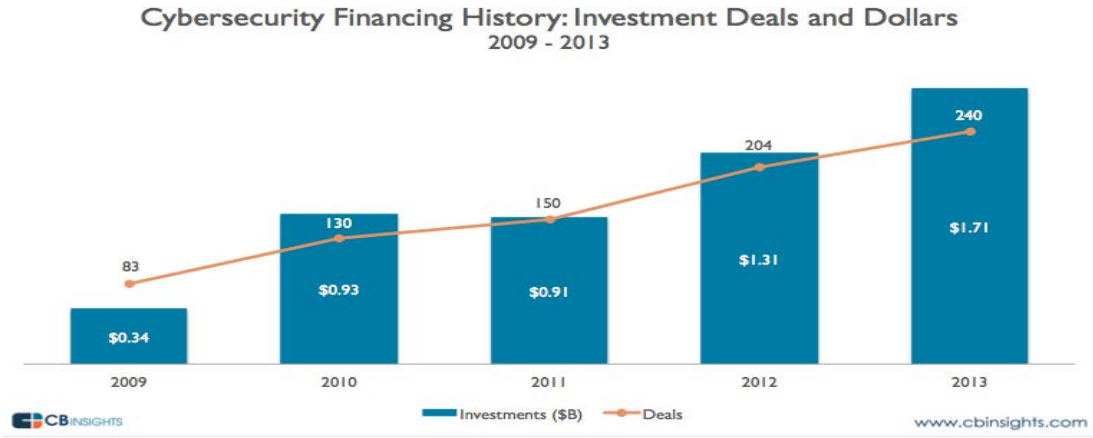
米国企業のNISTフレームワークの実施状況

出典：2014年　PwC社とｶｰﾈｷﾞｰﾒﾛﾝ大学の共同実施調査（全米約500社を対象）

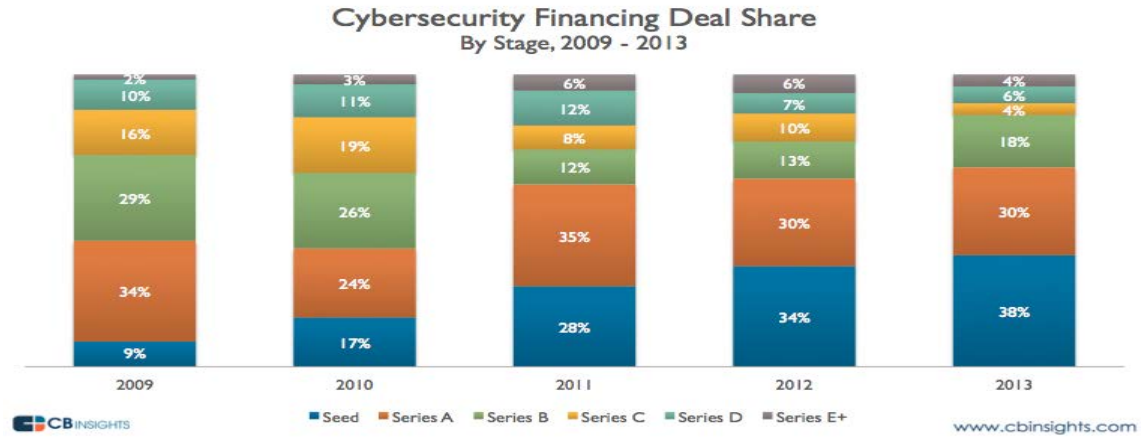
フレームワークコアの項目	フレームワーク実施率の平均値	個別項目毎の実施率（最高値と最低値）
特定 (Identify)	35%	81%：ｻｲﾊﾞｰリスクを含むリスク管理ﾌﾟﾛｸﾞﾗﾑを持つ 8%：ｻﾌﾟﾗｲﾁｪｰﾝのリスク管理
防御 (Protect)	40%	59%：ｱｶｳﾝﾄやﾊﾟｽﾜｰﾄﾞの管理規定を持つ 20%：問題時にまず対応するｵﾝｻｲﾄｻｰﾋﾞｽ者がいる
検知 (Detect)	40%	62%：侵入の検知ｼｽﾃﾑの導入 26%：ｾｷｭﾘﾃｨ関連情報･ｲﾍﾞﾝﾄを管理する技術の導入
対応 (Respond)	30%	54%：ｻｲﾊﾞｰ問題発生中・発生後の対応計画の実施 15%：地域の法執行機関（地元警察等）との協力
復旧 (Recover)	37%	53%：学んだ教訓を生かすｼｽﾃﾑを持つ 20%：PRや危機管理等で満足できる外部関係者を持つ

サイバーセキュリティ企業に対する投資

世界のサイバーセキュリティ関連ベンチャーへの投資額は、2009年から2013年の5年間で計52億ドル。2013年だけで17.1億ドル。投資件数も83件（09年）→240件（13年）に急増



サイバーセキュリティ関連ベンチャーへの投資は、特に初期ステージでの投資が多い
下記グラフの青部分（シードステージ；起業直後）とオレンジ部分（シリーズAステージ(起業後に最初に投資を受ける段階）で投資件数の約70%を占める



サイバーセキュリティクラスター

サイバーセキュリティクラスター

サイバー関連の研究・実務を行う省庁が民間活力を活用するため、サイバーセキュリティ関連企業と協力を活発化

→連邦省庁が集中するワシントンDC周辺にサイバーセキュリティ企業が集積
州政府も新しい企業育成を支援

●メリーランド州

（国家安全保障局（NSA）、米サイバー軍（USCYBERCOM）、国立標準技術研究所（NIST）等）

州政府の取り組み：

・民間セクターのサイバーセキュリティ市場開拓のため企業誘致（Luminal社に60万ドル支援）

・Cyber Maryland Conferenceの開催（講演会、求人フェア、競技会、ネットワーク構築など）

●バージニア州

（国防総省（DoD）、国土安全保障省（DHS）など）

州政府の取り組み：

・ベンチャーの立ち上げ支援のアクセラレーターを支援（MACH37社を通じ最大5万ドル支援）
起業後は製品開発・ビジネス展開のためのネットワーク紹介
（支援を受けた起業はバージニア州を拠点にすることが条件）

米国のサイバー保険

●米国のサイバー保険市場規模は、約20億ドル
・2014年以前は35－50%増に対し、2014年は2～3倍増との見込み。
・急増が見込まれるのは製造業、ライフサイエンス、食料品、公益事業など。
・損害保険と複数のサイバー保険に加入することで、トータルでサイバー被害をカバーしようとする米国企業が多い。
（ITTA社調べ（2014年）では、ヘルスケア、小売り、技術、情報通信分野で、75－80%の大企業が何かしらのサイバー保険に加入）

●NISTフレームワークは共通のリスク評価指標
・保険会社は、NISTのフレームワークを、各企業のリスクや、サプライチェーンにおける外部脅威に対する環境を知る指標として活用
・このような状況を受け、企業側もフレームワークを積極的に導入
（フレームワークは重要インフラ向けだが、内容は一般的なので他業種でも適用可能な内容）

●国土安全保障省（DHS）は、中小企業がフレームワークを効率よく導入するための方策について研究を開始

米国の主なサイバー保険

米国各社のサイバー保険は、多少の違いはあるもの、基本的な内容は似ている。

会社名	顧客規模（売上(ﾄﾞﾙ)）	平均掛け金	補償額	特徴
AIG保険	小企業（<2500万 中企業（2500万-10億） 大企業（>10億）	3000ドル 4万ドル 50万ドル	10万～50万ドル 100万～500万ドル 500万～1500万ドル	リスクマネージのツール等を提供
リバティ保険	中企業 大企業		100万～400万ドル 400万～1000万ドル	IT企業への保険も積極的
ハートフォード保険	中企業（<2億） 大企業（>2億）		最高1000万ドル	
ビーズリー保険	小企業（<3500万） 中企業（3500万-10億） 大企業（>10億）	1000ドル以下 5万ドル リスクに応じて	50万ドル 400万ドル 500万～1500万ドル	中小企業も重視

米国のサイバー保険の状況

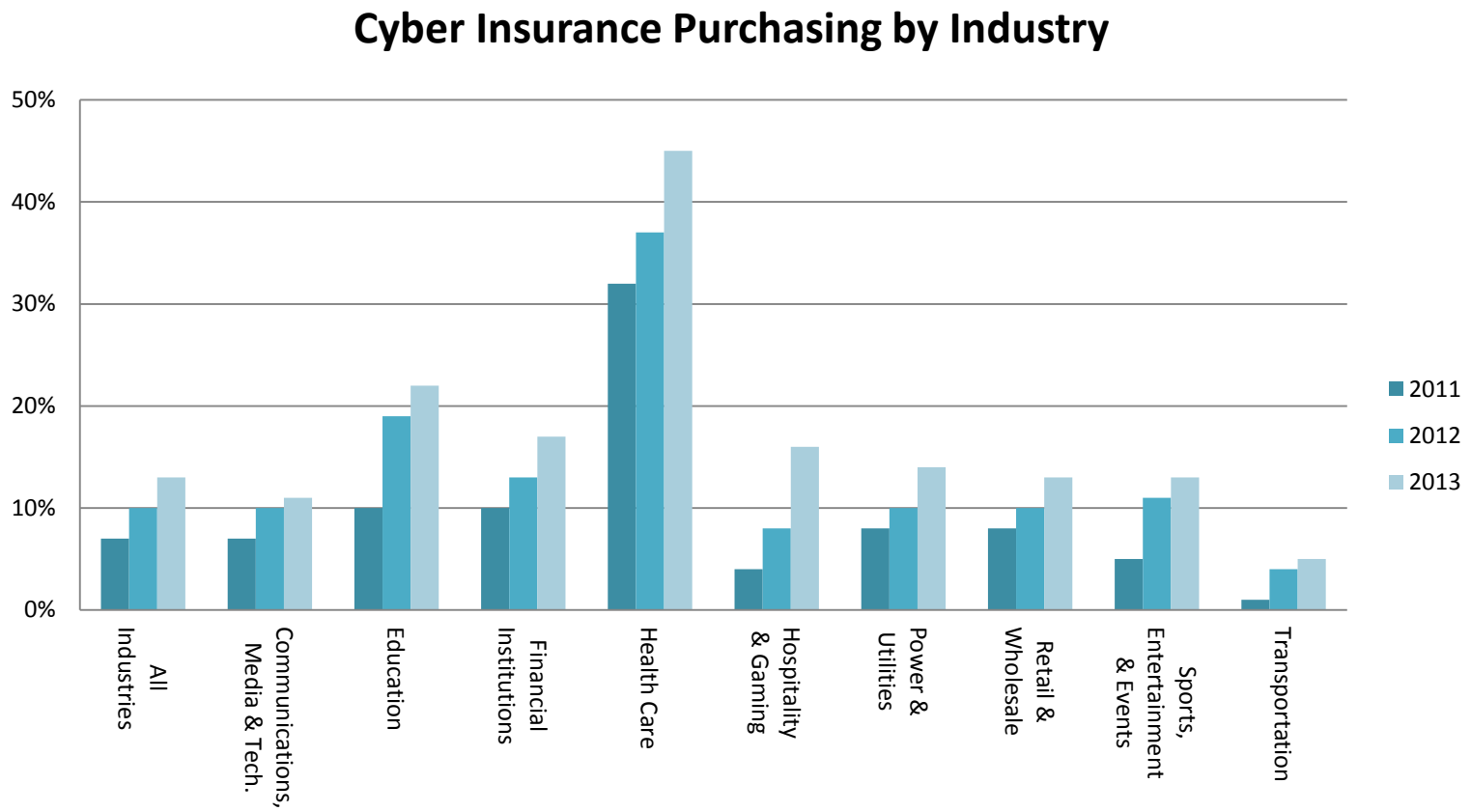
●マーシュ社が米国の顧客を対象にした調査によると、
中企業；　掛け金11～15万ドル、保険上限の合計（複数社）1000万ドル
大企業；　掛け金　平均250万ドル、保険上限の合計（複数社）1億ドル
（小企業のデータは少ないが、掛け金は平均2000ドル以下）

●各保険会社は、政府や各ベンダーからセキュリティ最新情報を得て、顧客に提供・アドバイスサービスの実施

●保険会社は業種・事業内容や企業規模ごとにリスクを評価
・IT企業などはリスクが高い業種と考えている。
保険会社にとって、各情報の機微さも重要な要素
・最も機微と感じるデータは、病院、ヘルスケア業界が持つ医療情報
・その他の機微な情報
小売業界　→クレジットカード情報など
製造業　→比較的機微な情報は少ないが、取引先企業情報など

米国の業種別サイバー保険加入率

マーシュ・リスク・マネージメント社の顧客（約400社）を対象にした調査によると、サイバー保険加入の割合は、全業種平均で約12%。最も高いのがヘルスケアセクターで約45%

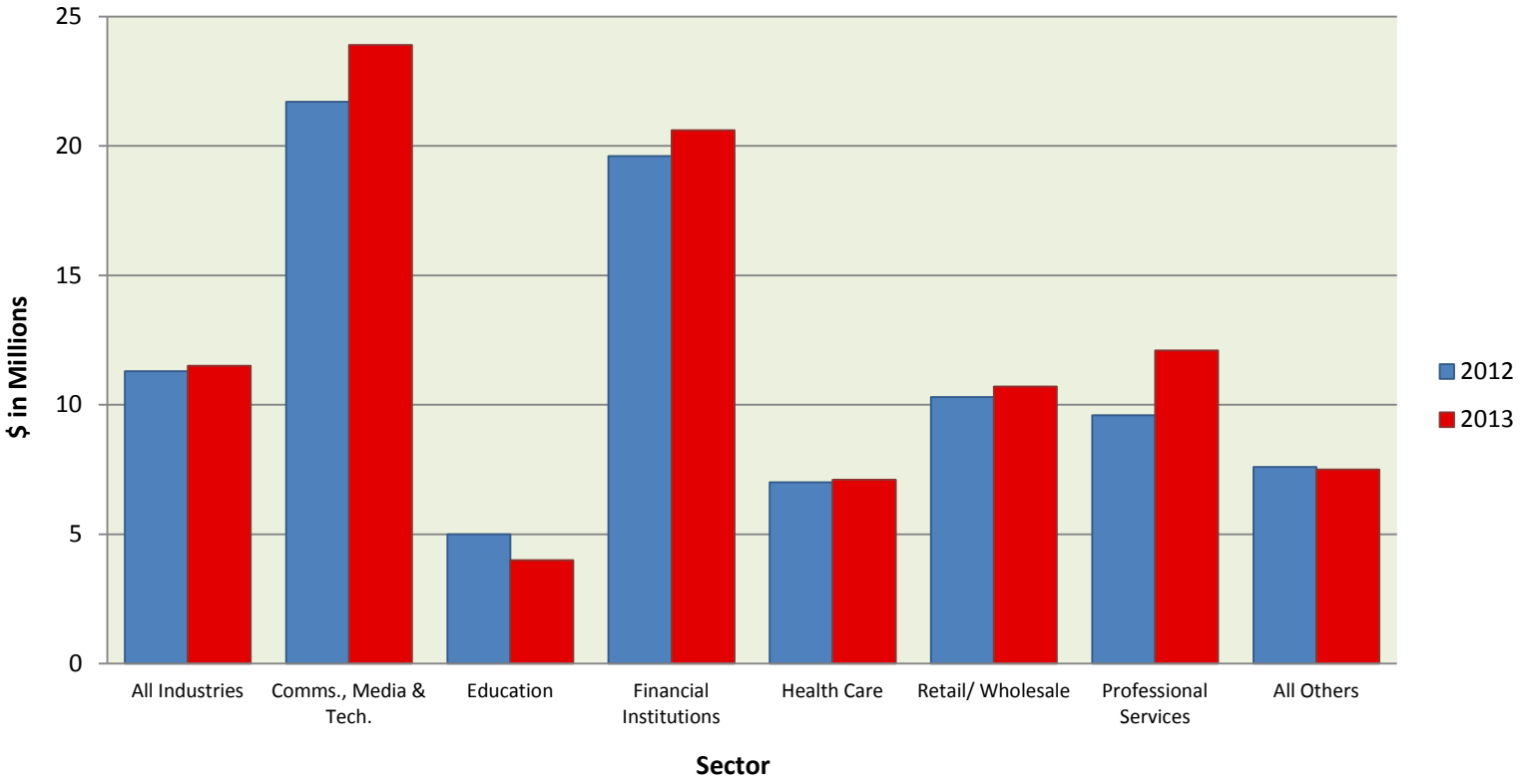


Source: *A Cybersecurity Call to Action,* MARSH and the Chertoff Group, November 2014

業種別サイバー保険の上限額

マーシュ・リスク・マネージメント社の顧客を対象にした調査によると、平均の保険金額（サイバー保険のみ）は、2012年の1130万(約13.5億円)ドル、2013年は1150万ドル（約13.8億円）。

各社が加入しているサイバー保険の合計上限額



出典：Benchmarking Trends: Interest in Cyber Insurance Continues to Climb, Marsh Risk Management Research Briefing, April 2014